

On self-dual double negacirculant codes

Adel Alahmadi*, Hatoon Shoaib†, Patrick Solé‡

Abstract

Double negacirculant (DN) codes are the analogues in odd characteristic of double circulant codes. Self-dual DN codes of odd dimension are shown to be consta-dihedral. Exact counting formulae are derived for DN codes. The special class of length a power of two is studied by means of Dickson polynomials, and is shown to contain families of codes with relative distances satisfying a modified Gilbert-Varshamov bound.

Key Words: quasi-twisted codes, dihedral group, Dickson polynomials

MSC(2010): 94 B25, 05 E30

1 Introduction

A matrix A over a finite field \mathbb{F}_q is said to be *negacirculant* if its rows are obtained by successive negashifts from the first row. A *negashift* maps the vector $(x_0, \dots, x_{n-1}) \in \mathbb{F}_q^n$ to $(-x_{n-1}, x_0, \dots, x_{n-2})$.

In this paper we consider *double negacirculant* (DN) codes over finite fields, that is $[2n, n]$ codes with generator matrices of the shape (I, A) with I the identity matrix of size n and A a negacirculant matrix of order n . For instance, the famous *tetracode*, a self-dual MDS ternary code of length 4 [5] is DN. This construction was introduced in [8] under the name *quasi-twisted code*. We prefer to reserve this term for the more general class of codes described in [19]. A code of length N is quasi-twisted of index ℓ for $\ell \mid N$, and co-index $m = \frac{N}{\ell}$ if it is invariant under the power T_α^ℓ of the *constashift* T_α defined as

$$T_\alpha : (x_0, \dots, x_{N-1}) \mapsto (\alpha x_{N-1}, x_0, \dots, x_{N-2}).$$

*Math Dept, King Abdulaziz University, Jeddah, Saudi Arabia, Email: adelnife2@yahoo.com

†Math Dept, King Abdulaziz University, Jeddah, Saudi Arabia, Email: hashoaib@kau.edu.sa

‡CNRS/LTCL, Telecom ParisTech, Université de Paris-Saclay, 75 013 Paris, France & Math. Dept, King Abdulaziz University, Jeddah, Saudi Arabia. Email: sole@enst.fr

Such a code affords a natural structure of module over the auxiliary ring

$$R(m, \mathbb{F}_q) = \frac{\mathbb{F}_q[x]}{(x^m - \alpha)}.$$

In other words, it can be regarded as a code of length ℓ over the ring $R(m, \mathbb{F}_q)$. An algebraic way to study such a code is to decompose the semilocal ring $R(m, \mathbb{F}_q)$ as a direct sum of local rings by the Chinese Remainder Theorem [19], thus following the approach initiated for quasi-cyclic codes in [11]. The benefit of this technique is to reduce the study of QT codes to that of shorter codes over larger alphabets. Besides, the study of duality is made transparent, thus allowing the construction of self-dual QT codes, as in, for instance, [19]. The number of rings occurring in the decomposition of $R(m, \mathbb{F}_q)$ equals the number of irreducible factors of $x^m - a$. In the following section we focus on self-dual DN codes. These have been explored numerically in [6, 7]. First, we show that such codes are consta-dihedral, in the sense that they are invariant under a monomial representation of the dihedral group of order $2n$. This definition is related to but different from that of [16]. Next, we specialize further by assuming that n is a power of two. For some specific alphabets, it can be shown that in that case $x^n + 1$ can be factored into a product of two irreducible polynomials [14, 10]. This is a favorable situation to apply the Chinese Remainder Theorem approach of [11, 19], as the decomposition of $R(m, \mathbb{F}_q)$ contains only two terms. It allows to derive exact enumeration formulae and, from there, using the so-called expurgated random coding technique, to give an asymptotic lower bound on the minimum distance of these DN codes. This is an analogue of the Varshamov Gilbert bound. Other similar asymptotic estimates use non constructive lengths and factorization of $x^n + 1$ [4, 2]. The analogous result on double circulant codes in even characteristic relies on Artin conjecture [3], or an intricate induction [9].

The material is organized as follows. The next section collects the necessary notions and notations. Section 3 studies the automorphism group of these codes. Section 4 derives the factorization of $x^n + 1$ over \mathbb{F}_q when n is a power of 2 and q is odd. Section 5 contains enumeration formulae and asymptotics. Section 6 concludes the article and points the way to some challenging open problems.

2 Definitions and notation

2.1 Codes

Let \mathbb{F}_q denote the finite field of order q . We assume throughout that q is odd. In the following, we will consider codes over \mathbb{F}_q of length $2n$ with n odd and coprime to q . Their generator matrix G will be of the form $G = (I, A)$ where I is the identity matrix of order n and A is an $(n \times n)$ -negacirculant matrix. We call such codes *double negacirculant* (DN) codes. We will denote by \mathcal{C}_a the DN code with first row of A being the x -expansion of a in the ring $R(n, \mathbb{F}_q)$.

If $C(n)$ is a family of codes of parameters $[n, k_n, d_n]$, the *rate* R and *relative distance* δ are defined as

$$R = \limsup_{n \rightarrow \infty} \frac{k_n}{n},$$

and

$$\delta = \liminf_{n \rightarrow \infty} \frac{d_n}{n}.$$

Both limits are finite as limits of bounded quantities. Such a family of codes is said to be *good* if $R\delta \neq 0$.

Recall the q -ary *entropy function* defined for $0 < x < \frac{q-1}{q}$ by

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$

This quantity is instrumental in the estimation of the volume of high-dimensional Hamming balls when the base field is \mathbb{F}_q . The result we are using is that the volume of the Hamming ball of radius xn is, up to subexponential terms, $q^{nH_q(x)}$, when $0 < x < 1$ and n goes to infinity [5, Lemma 2.10.3].

2.2 Groups

The *symmetric* group S_n is the group of permutations of n objects. The *dihedral* group \mathcal{D}_n , is defined as the unique group of order $2n$ on two generators r and s of respective orders n and 2 and satisfying the relation $srs = r^{-1}$. A code of length $2n$ is called *dihedral* if it is invariant under \mathcal{D}_n acting transitively on its coordinate places.

Recall that a *monomial* matrix over \mathbb{F}_q of order g has exactly one nonzero element per row and per column. The monomial matrices form a group $M(g, q)$ of order $g!(q-1)^g$ under multiplication. This group is abstractly isomorphic to the wreath product $\mathbb{Z}_{q-1} \wr S_g$.

By a *monomial representation* of a group G over \mathbb{F}_q we shall mean a group morphism from G into $M(g, q)$. A code of length $2n$ will be said to be *consta-dihedral* if it is held invariant under right multiplication by a monomial representation of the dihedral group \mathcal{D}_n . An alternative, but related definition can be found in [16].

2.3 Polynomials

The *Dickson polynomial* (of the first kind) are given by $D_0(x, \alpha) = 2$, and for $n > 0$, by

$$D_n(x, \alpha) = \sum_{p=0}^{\lfloor n/2 \rfloor} \frac{n}{n-p} \binom{n-p}{p} (-\alpha)^p x^{n-2p}.$$

The D_n satisfy the identity

$$D_n(u + \alpha/u, \alpha) = u^n + (\alpha/u)^n.$$

3 Symmetry

Let $M_n(q)$ denote the set of all $n \times n$ matrices over \mathbb{F}_q .

Lemma 1 *Let A be an $(n \times n)$ -negacirculant matrix over \mathbb{F}_q . Then there exists an $(n \times n)$ -generalized permutation matrix P such that $PAP = A^T$.*

Proof. Consider the following permutation is S_n :

$$\pi = (2, n)(3, n-1) \dots \left(\frac{n-1}{2}, \frac{n+5}{2}\right) \left(\frac{n+1}{2}, \frac{n+3}{2}\right).$$

Then the generalized permutation matrix P_π corresponding to the permutation π , is

$$P_\pi = \begin{pmatrix} e_{\pi(1)} \\ e_{\pi(2)} \\ \cdot \\ \cdot \\ \cdot \\ e_{\pi(n)} \end{pmatrix} = \begin{pmatrix} e_1 \\ e_n \\ \cdot \\ \cdot \\ \cdot \\ e_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & \alpha \\ 0 & 0 & \dots & \alpha & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & \alpha & \dots & 0 & 0 \end{pmatrix} = P$$

where $\alpha^2 = 1$. Then it easy to observe that, $PAP = A^T$.

□

Theorem 2 *For $n \geq 3$, and q odd, every self-dual quasi twisted code \mathcal{C} of length $2n$ over \mathbb{F}_q is consta-dihedral.*

Proof. Let C be a self-dual double negacirculant code of length $2n$ with generator matrix $G = (I, A)$ with A negacirculant and $AA^T = -I$. Computing $A^T G = (A^T, -I)$ and conjugating by P of Lemma 1 we get $PA^T GP = (A, -I)$. Define the antiswap involution s by the rule $s(x, y) = s(y, -x)$, where x, y are vectors of length n over \mathbb{F}_q . Note that $s^2 = 1$. Clearly $s \in M(2n, q)$. Thus $\pi s \in M(2n, q)$ and it preserves C . A monomial representation of \mathcal{D}_n is then $\langle \tau, \pi s \rangle$. Thus C is consta-dihedral. □

4 Factorizations

The complete factorization of $x^{2^n} + 1$ over \mathbb{F}_q with $q \equiv 3 \pmod{4}$ is given in the following theorem [14].

Theorem 3 *Let $q \equiv 3 \pmod{4}$, where $q = 2^A m - 1$, $A \geq 2$, m is odd integer. Let $n \geq 2$,*

(a) If $n < A$, then $x^{2^n} + 1$ is the product of 2^{n-1} irreducible trinomials over \mathbb{F}_q

$$x^{2^n} + 1 = \prod_{\gamma \in \Gamma} (x^2 + \gamma x + 1),$$

where Γ is the set of all roots of $D_{2^{n-1}}(x, 1)$.

(b) If $n \geq A$, then $x^{2^n} + 1$ is the product of 2^{A-1} irreducible trinomials over \mathbb{F}_q

$$x^{2^n} + 1 = \prod_{\delta \in \Delta} (x^{n-A+1} + \delta x^{n-A} - 1),$$

where Δ is the set of all roots of $D_{2^{A-1}}(x, -1)$ in \mathbb{F}_q .

Example 1 If $q = 3$ i.e. $q \equiv 3 \pmod{4}$, then $q = 2^2 \cdot 1 - 1$ implies that $A = 2$, $m = 1$, and $D_2(x, -1) = \{1, 2\}$, then by Theorem 3:

$$x^{2^n} + 1 = (x^{2^{n-1}} + x^{2^{n-2}} + 2)(x^{2^{n-1}} + 2x^{2^{n-2}} + 2)$$

We need the analogous factorization theorem when $q \equiv 1 \pmod{4}$. We prepare for the proof by an arithmetic Lemma. If r, s are two integers, we denote by $\text{ord}_r(s)$ the smallest integer i such that $s^i \equiv 1 \pmod{r}$.

Lemma 4 If $q = 2^{A+1}m + 1$, with m , odd and A integer, then $\text{ord}_{2^{n+1}}(q) = 2^{n-A}$.

Proof. We derive

$$q^{2^{n-A}} \equiv 1 \pmod{2^{n+1}} \quad (1)$$

by induction on n .

For $n = A+1$, note that, by definition, $q \equiv 1 \pmod{2^{A+1}}$, implying $q^2 \equiv 1 \pmod{2^{A+2}}$. Therefore (1) is true for $n = A+1$.

Assume that (1) is true for $n = k + A + 1$, then we have $q^{2^{k+1}} = 1 + \beta 2^{A+k+2}$, for some integer β , and squaring, we get $q^{2^{k+2}} = 1 + 2\beta 2^{A+k+2} + \beta^2 2^{2A+k+2}$, which implies (1) for $n = k + A + 2$. This shows that $\text{ord}_{2^{n+1}}(q)$ is a power of two dividing 2^{n-A} . Using a similar induction on n it can be shown that

$$q^{2^{n-A-1}} \equiv 1 + 2^n \pmod{2^{n+1}}.$$

Hence $\text{ord}_{2^{n+1}}(q) = 2^{n-A}$. □

Theorem 5 Let $q \equiv 1 \pmod{4}$, where $q = 2^A m + 1$, $A \geq 2$, m is odd integer. Denote by U_k is the set of all primitive 2^k th roots of unity in \mathbb{F}_q . If $n \geq 2$, then

(a) If $n \leq A$, then $\text{ord}_{2^{n+1}}(q) = 1$ and $x^{2^n} + 1$ is the product of 2^n linear factors over \mathbb{F}_q

$$x^{2^n} + 1 = \prod_{u \in U_{n+1}} (x + u).$$

(b) If $n \geq A+1$, then $\text{ord}_{2^{n+1}}(q) = 2^{n-A}$ and $x^{2^n} + 1$ is the product of 2^A irreducible binomials over \mathbb{F}_q of degree 2^{n-A}

$$x^{2^n} + 1 = \prod_{u \in U_{A+1}} (x^{2^{n-A}} + u).$$

Proof. (a) In this case, $q \equiv 1 \pmod{2^{n+1}}$, we can apply [10, theorem 2.47], with $d = 1$. (b) If $n \geq A + 1$, then to apply [10, theorem 2.47], knowing that $\phi(2^{n+1}) = 2^n$ and $d|2^n$, we use Lemma 4 to prove that $\text{ord}_{2^{n+1}}(q) = 2^{n-A}$ so that we can take $d = 2^{n-A}$, and therefore that $x^{2^n} + 1$ is the product of 2^A irreducible polynomials over \mathbb{F}_q of degree 2^{n-A} .

Writing this identity for $n = A$ by (a) where the factors are linear and substituting $x = x^{2^{n-A}}$, we obtain a factorization of 2^A binomials over \mathbb{F}_q , each of degree 2^{n-A} . They can be shown to be irreducible by application of [10, th. 3.75]. The result follows. \square

Example 2 If $q = 5$ i.e. $q \equiv 1 \pmod{4}$, then $q = 2^2 \cdot 1 + 1$ implies that $A = 1$, $m = 1$, and $U_2 = \{2, 3\}$, then by Theorem 5:

$$x^{2^n} + 1 = (x^{2^{n-1}} + 2)(x^{2^{n-1}} + 3).$$

5 Asymptotics

5.1 Enumeration

The following result is not needed in its full generality for the asymptotic application, but is of interest in its own right. It can be viewed as enumerating negacirculant matrices of order n .

Proposition 6 Let n be an integer, and q a prime power coprime with n . Suppose, if n is odd, that -1 is a square in \mathbb{F}_q . Assume that the factorization of $x^n + 1$ into irreducible polynomials over \mathbb{F}_q is of the form

$$x^n + 1 = \alpha \prod_{j=1}^s g_j(x) \prod_{j=1}^t h_j(x) h_j^*(x),$$

with $\alpha \in \mathbb{F}_q$, $n = s + 2t$ and g_j a self-reciprocal polynomial of degree $2d_j$, the polynomial h_j is of degree e_j and $*$ denotes reciprocation. If n is odd, then let $g_1 = x + 1$. The number of self-dual double negacirculant codes over \mathbb{F}_q is then

$$2 \prod_{j=2}^s (1 + q^{d_j}) \prod_{j=1}^t (q^{e_j} - 1)$$

if n is odd

$$\prod_{j=1}^s (1 + q^{d_j}) \prod_{j=1}^t (q^{e_j} - 1)$$

if n is even.

Proof. (sketch) We use the Chinese Remainder Theorem decomposition of $R(n, \mathbb{F}_q)$, as explained in the Introduction. If n is odd and \mathbb{F}_q contains a square root of -1 , say ω , then the factor $g_1 = x + 1$ of $x^n + 1$ yields a term \mathbb{F}_q in that decomposition. There are two self-dual codes of length 2 over \mathbb{F}_q that is $\langle [1, \omega] \rangle$, and $\langle [1, -\omega] \rangle$. More generally, a factor g_i of degree $2d_i$ leads to counting self dual hermitian codes of length 2 over $\mathbb{F}_{q^{2d_i}}$, that is to count the solutions of the equation $1 + x^{1+q^{d_i}} = 0$ over that field. Using the existence of a root of order $q^{2d_i} - 1$, it can be seen that this equation has $1 + q^{d_i}$ solutions. Alternatively, one could specialize the formulae in [15].

In the case of reciprocal pairs (h_j, h_j^*) , note that the number of linear codes of length 2 over some \mathbb{F}_Q admitting, along with their duals, a systematic form is $Q - 1$, all of dimension 1. Indeed their generator matrix is of the form $[1, u]$ with u nonzero. We conclude by letting $Q = q^{e_j}$.

□

5.2 Distance bounds

In this section, we assume that q is such that $x^n + 1$, for n a power of 2, has only two irreducible factors, say h' and h'' , and that they are reciprocal of each other. For convenience, let $K' = \frac{\mathbb{F}_q[x]}{(h')}$ and $K'' = \frac{\mathbb{F}_q[x]}{(h'')}$. These two fields are both isomorphic to $\mathbb{F}_{q^{n/2}}$. By Theorems 3 and 5, this is the case if $q = 4m \pm 1$, with m odd. For instance this happens if $q = 3, 5$ but not if $q = 7$.

Lemma 7 *If $u \neq 0$ has Hamming weight $< n$, there are at most $q^{\frac{n}{2}}$ polynomials a such that $u \in \mathcal{C}_a = \langle [1, a] \rangle$, and at most one polynomial a such that $u \in \mathcal{C}_a$ and \mathcal{C}_a is self dual.*

Proof. Let $\mathcal{C}_a = \langle [1, a] \rangle$, and let $u = (c, d)$, with c, d of length n . The condition $u \in \mathcal{C}_a$ is equivalent to the equations,

$$d' = a'c' \quad \text{over } K'$$

$$d'' = a''c'' \quad \text{over } K''$$

Then we have:

- (I) If \mathcal{C}_a is self dual, then $\langle [1, a'] \rangle = \langle [1, a''] \rangle^\perp$ implies $1 + a'a'' = 0$
 If $d' = c' = 0$, then a' is undetermined, and if $c'', d'' \neq 0$, then $a'' = \frac{d''}{c''}$ that implies a' determined and $a' = -\frac{1}{a''}$. Hence, for given $u = (c, d)$, there is at most one choice for a .
- (II) If \mathcal{C}_a is not necessarily self dual then, we have two cases:
 - (i) If $c' \neq 0$, then $a' = \frac{d'}{c'}$ has a unique solution.

- (ii) If $c' = 0$, then
 - (a) If $d' \neq 0$, then we have no solution.
 - (b) If $d' = 0$, then a' is undetermined i.e. we have $q^{\frac{n}{2}}$ choices for a' .

Similarly, we have the same solutions for a'' :

- (i) If $c'' \neq 0$, then $a'' = \frac{d''}{c''}$ has a unique solution.
- (ii) If $c'' = 0$, then
 - (a) If $d'' \neq 0$, then we have no solution.
 - (b) If $d'' = 0$, then a'' is undetermined i.e. we have $q^{\frac{n}{2}}$ choices for a'' .

Hence, for given $u = (c, d)$, there is at most $q^{\frac{n}{2}}$ choices for a .

□

We are now ready for the main result of this paper.

Theorem 8 *If q is odd integer, and n is a power of 2, then there are infinite families of:*

- (i) *double negacirculant codes of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{4}$.*
- (ii) *self dual double negacirculant codes of relative distance δ satisfying $H_q(\delta) \geq \frac{1}{4}$.*

Proof. (i) The double negacirculant codes containing a vector of weight $d \sim \delta n$ or less are by standard entropic estimates and Lemma 7 of the order $q^{\frac{n}{2}} \times q^{2nH_q(\delta)}$, up to subexponential terms. This number will be less than the total number of double negacirculant codes which is by Proposition 6 of the order of q^n .

(ii) The double negacirculant codes containing a vector of weight $d \sim \delta n$ or less are by standard entropic estimates and Lemma 7 of the order $1 \times q^{2nH_q(\delta)}$, up to subexponential terms. This number will be less than the total number of self dual double negacirculant codes which is by Proposition 6 of the order of $q^{\frac{n}{2}}$. □

6 Conclusion

In this paper, we have considered double negacirculant codes. As noted in [6], they are an alternative to double circulant (DC) self-dual codes over some fields where DC do not exist. By an old result of [18], a DC self-dual code does not exist over fields like \mathbb{F}_3 where -1 is not a square. This paper can thus be considered as a companion paper of [1]. The main difference between the two papers is that a factorization of $x^n + 1$ into two irreducible polynomials is easier and more elementary to find than a factorization of $x^n - 1$ into two irreducible polynomials which requires n to be a prime for which 2 is primitive. The existence of infinitely many such n 's requires the truth of Artin's conjecture [14]. Thus the present paper is more explicit and more elementary than [1].

Many questions remain open. The DN codes can be construed as QT codes of index 2. In view of the constructions of [7], it would be of interest to consider quasi-twisted codes of index 4. At a technical level, it would be interesting to generalize Lemma 7 to fields \mathbb{F}_q with q 's like $q = 7$, where the factorization of $x^n + 1$ for n a power of 2, contains four polynomials or more. More generally, in view of the existence of self-dual quasi-twisted codes for the hermitian product [17], generalizing our asymptotics result to that setting is a possibility.

References

- [1] A. Alahmadi, F. Ozdemir, P. Solé, On self-dual double circulant codes, submitted.
- [2] L.M.J. Bazzi, S.K. Mitter, Some randomized code constructions from group actions, *IEEE Trans. Inform. Theory* (2006) 3210–3219.
- [3] C.L. Chen, W.W. Peterson, E.J. Weldon, Some results on quasi-cyclic codes, *Information and Control* (1969) 407–423.
- [4] V.Chepyzhov, A Varshamov-Gilbert bound for quasi-twisted codes of rate $\frac{1}{n}$, *Proceedings of the joint Swedish-Russian International workshop on Information Theory, Mölle, Sweden* (1993) 214–218.
- [5] W. Cary Huffman and Vera Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, (2003).
- [6] T. Aaron Gulliver, M. Harada, and Hiroki Miyabayashi, Double circulant and quasi-twisted self-dual codes over \mathbb{F}_5 and \mathbb{F}_7 , *Advances Math. Communications* 1 (2007), 223–238.
- [7] M. Harada, W. Holzmann, H. Kharaghani and M. Khorvash, Extremal ternary self-dual codes constructed from negacirculant matrices, *Graphs Combin.* 23 (2007), 401–417.
- [8] R. Hill, P. Greenough, Optimal quasi-twisted codes, *Proc. Intern. Workshp of Comb. Cod. and Crypt.*, Bulgaria (1992).
- [9] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$ " *IEEE Trans. Inform. Theory*, (1974) 674.
- [10] R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA (1983).
- [11] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Trans. Inform. Theory* (2001) 2751–2760.
- [12] S. Ling, P. Solé, Good self-dual quasi-cyclic codes exist, *IEEE Trans. Inform. Theory* (2003) 1052–1053

- [13] P. Moree, Artin's primitive root conjecture—a survey, *Integers* 10 (6) (2012) 1305–1416.
- [14] H. Meyn, Factorization of the cyclotomic polynomial $x^{2^n} + 1$ over finite fields, *Finite Fields and their Applications* (1996) 439–442.
- [15] E.M. Rains, N.J.A. Sloane, Self-dual codes, pp. 117–294, in *Handbook of Coding Theory*, W.C. Huffman, V. Pless, eds., North-Holland (1998).
- [16] V. Shashidar, B. S. Rajan, Consta-dihedral codes and their transform domain characterization, ISIT 2004, p.256, IEEE Press.
- [17] E. Sangwisut, S. Jitman, P. Udomkavanich, Constacyclic and quasi-twisted hermitian self-dual codes over finite fields, arxiv (2016).
- [18] M. Ventou, C. Rigoni, Self-dual double circulant codes, *Discrete Math* 56 (1985) 291–298.
- [19] J. Yan, On quasi-twisted codes over finite fields, *Finite Fields and their Applications* 18 (2012) 237–257.